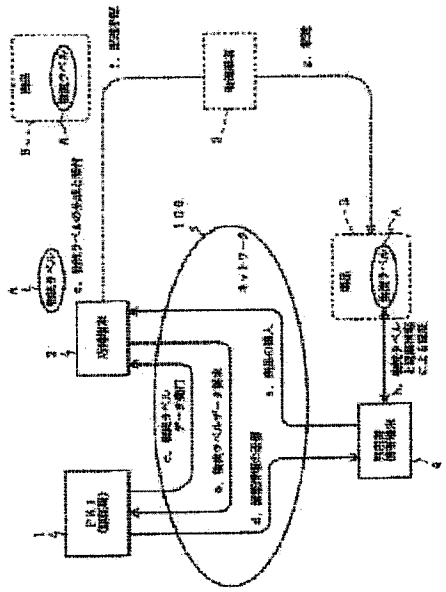
LOGISTICS PKI SERVICE SYSTEM, PORTABLE TERMINAL, AND LOGISTIC PKI SERVICE METHOD USED THEREFOR

Publication number: JP2003223493 (A)
Publication date: 2003-08-08
Inventor(s): KATAYAMA TORU; YOSHIDA YOSHINORI +
Applicant(s): NEC CORP +
Classification:
- international: ***B65G61/00; G06K1/12; G06K17/00; G06K19/00; G06K19/10; G06K7/00; G06Q10/00; G06Q20/00; G06Q50/00; G09F3/00; H04L9/32;*** **B65G61/00; G06K1/00; G06K17/00; G06K19/00; G06K19/10; G06K7/00; G06Q10/00; G06Q20/00; G06Q50/00; G09F3/00; H04L9/32;** (IPC1-7): B65G61/00; G06F17/60; G06K1/12; G06K17/00; G06K19/00; G06K19/10; G06K7/00; G09F3/00; H04L9/32
- European: G06Q10/00D; G06Q20/00; G06Q20/00K1; G06Q20/00K3B; G06Q20/00K5
Application number: JP20020020841 20020130
Priority number(s): JP20020020841 20020130

Also published as:
US2003144968 (A1)
US2008109247 (A1)
US2008183482 (A1)

Abstract of **JP 2003223493 (A)**

PROBLEM TO BE SOLVED: To provide a logistic PKI (Public key Infrastructure) service system capable of improving reliability and safety in a physical distribution part. ; SOLUTION: When an article released from a portable terminal 4 of a user to a store terminal 2 via a network 1000 is purchased, the store terminal 2 receives physical distribution label data issued from PKI 1 and the portable terminal of the user receives an identification information transmitted from the PKI 1. The store terminal 2 produces a physical distribution label A based on the physical distribution label data from the PKI 1, attaches the physical distribution label A to the article B, and requests the delivery of the article B to a physical distribution agent 3. When the article B is delivered by the physical distribution agent 3, the portable terminal 4 of the user reads information of the physical distribution label A attached to the article B and identifies it by the information of the physical distribution label A and the identification information from the PKI 1. ; COPYRIGHT: (C)2003,JPO



Data supplied from the ***espacenet*** database — Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－223493
（P2003－223493A）
(43)公開日　平成15年８月８日(2003.8.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	１１４	Ｃ０６Ｆ　17/60	１１４	５Ｂ０３５
	５１２		５１２	５Ｂ０５８
Ｂ６５Ｇ　61/00	５２４	Ｂ６５Ｇ　61/00	５２４	５Ｂ０７２
	５５０		５５０	５Ｊ１０４
Ｇ０６Ｋ　1/12		Ｃ０６Ｋ　1/12	Ａ	

審査請求　未請求　請求項の数24　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願2002－20841(P2002－20841)

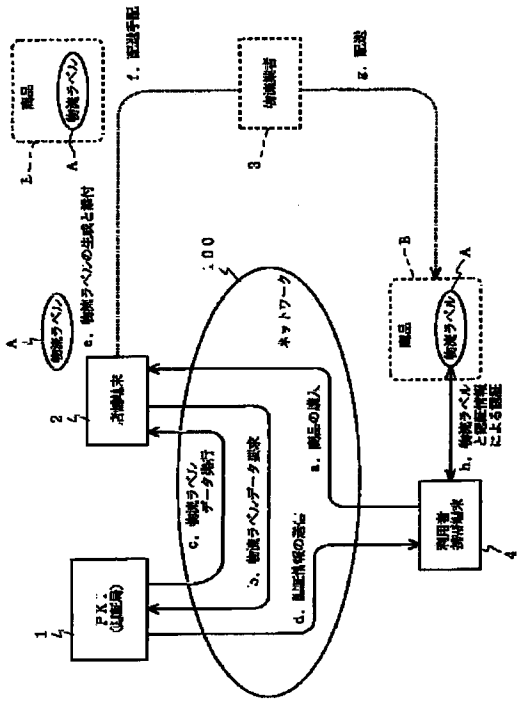
(22)出願日　平成14年１月30日(2002.1.30)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　片山　透
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　吉田　吉憲
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088812
弁理士　▲柳▼川　信

最終頁に続く

(54)【発明の名称】　ロジスティックＰＫＩサービスシステム、携帯端末及びそれに用いるロジスティックＰＫＩサービス方法

(57)【要約】
【課題】　物流部分における信頼性や安全性を向上可能なロジスティックＰＫＩサービスシステムを提供する。
【解決手段】　利用者の携帯端末４からネットワーク１００を介して店舗端末２に掲示された商品が購入されると、店舗端末２はＰＫＩ１から発行される物流ラベルデータを受取り、利用者の携帯端末４はＰＫＩ１から送信される認証情報を受信する。店舗端末２はＰＫＩ１からの物流ラベルデータに基づいて物流ラベルＡを生成し、その物流ラベルＡを商品Ｂに添付した後、商品Ｂの配送依頼を物流業者３に依頼する。利用者の携帯端末４は物流業者３によって商品Ｂが配送されると、商品Ｂに添付された物流ラベルＡの情報を読取り、物流ラベルＡの情報とＰＫＩ１からの認証情報とによる認証を行う。



【特許請求の範囲】

【請求項１】　配送物の配送時に当該配送物の情報を示すラベルデータを要求しかつ送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成する端末装置と、
前記端末装置からの要求に応答して前記ラベルデータと前記配送物の認証情報とを発行する認証局と、
配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行う携帯端末とを有することを特徴とするロジスティックＰＫＩサービスシステム。

【請求項２】　前記ラベルは、少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを示す情報を含むことを特徴とする請求項１記載のロジスティックＰＫＩサービスシステム。

【請求項３】　前記ラベルは、前記配送物の受取者の公開鍵で暗号化され、前記配送物の受取時に前記配送物の受取者の秘密鍵で復号されることを特徴とする請求項２記載のロジスティックＰＫＩサービスシステム。

【請求項４】　前記ラベルは、二次元バーコードとして印刷されることを特徴とする請求項２または請求項３記載のロジスティックＰＫＩサービスシステム。

【請求項５】　前記ラベルは、集積回路からなるタグであることを特徴とする請求項２または請求項３記載のロジスティックＰＫＩサービスシステム。

【請求項６】　前記認証局は、前記配送物の配送元を証明する電子署名を発行する手段と、前記配送物の依頼者を証明する電子署名を発行する手段とを含むことを特徴とする請求項１から請求項５のいずれか記載のロジスティックＰＫＩサービスシステム。

【請求項７】　前記携帯端末は、前記配送物の認証結果として少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを前記ラベルから復号して表示することを特徴とする請求項２から請求項５のいずれか記載のロジスティックＰＫＩサービスシステム。

【請求項８】　前記配送物の依頼者と前記配送物の受取者とが同一であることを特徴とする請求項１から請求項７のいずれか記載のロジスティックＰＫＩサービスシステム。

【請求項９】　前記配送物の依頼者と前記配送物の受取者とが異なることを特徴とする請求項１から請求項７のいずれか記載のロジスティックＰＫＩサービスシステム。

【請求項１０】　配送されてきた配送物に添付されている当該配送物の情報を示すラベルから読取った情報と認証局からの当該配送物の認証情報とによって認証を行う手段を有することを特徴とする携帯端末。

【請求項１１】　前記ラベルは、少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを示す情報を含むことを特徴とする請求項１０記載の携帯端末。

【請求項１２】　前記ラベルは、前記配送物の受取者の公開鍵で暗号化され、前記配送物の受取時に前記配送物の受取者の秘密鍵で復号されることを特徴とする請求項１１記載の携帯端末。

【請求項１３】　前記ラベルは、二次元バーコードとして印刷されることを特徴とする請求項１１または請求項１２記載の携帯端末。

【請求項１４】　前記ラベルは、集積回路からなるタグであることを特徴とする請求項１１または請求項１２記載の携帯端末。

【請求項１５】　前記配送物の認証結果として少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを前記ラベルから復号して表示するようにしたことを特徴とする請求項１１から請求項１４のいずれか記載の携帯端末。

【請求項１６】　端末装置において、配送物の配送時に当該配送物の情報を示すラベルデータを要求し、それに応答して送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成し、認証局において、前記端末装置からの要求に応答して前記ラベルデータと前記配送物の認証情報とを発行し、
携帯端末において、配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行うことを特徴とするロジスティックＰＫＩサービス方法。

【請求項１７】　前記ラベルは、少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを示す情報を含むことを特徴とする請求項１６記載のロジスティックＰＫＩサービス方法。

【請求項１８】　前記ラベルは、前記配送物の受取者の公開鍵で暗号化され、前記配送物の受取時に前記配送物の受取者の秘密鍵で復号されることを特徴とする請求項１７記載のロジスティックＰＫＩサービス方法。

【請求項１９】　前記ラベルは、二次元バーコードとして印刷されることを特徴とする請求項１７または請求項１８記載のロジスティックＰＫＩサービス方法。

【請求項２０】　前記ラベルは、集積回路からなるタグであることを特徴とする請求項１７または請求項１８記載のロジスティックＰＫＩサービス方法。

【請求項２１】　前記認証局において、前記配送物の配送元を証明する電子署名を発行し、前記配送物の依頼者を証明する電子署名を発行することを特徴とする請求項１６から請求項２０のいずれか記載のロジスティックＰＫＩサービス方法。

【請求項２２】　前記携帯端末において、前記配送物の認証結果として少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを前記ラベルから復号して表示することを特徴とする請求項１７から請求項２０のいずれか記載のロジスティックＰＫＩサービ

ス方法。

【請求項23】　前記配送物の依頼者と前記配送物の受取者とが同一であることを特徴とする請求項16から請求項22のいずれか記載のロジスティックPKIサービス方法。

【請求項24】　前記配送物の依頼者と前記配送物の受取者とが異なることを特徴とする請求項16から請求項22のいずれか記載のロジスティックPKIサービス方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はロジスティックPKIサービスシステム、携帯端末及びそれに用いるロジスティックPKIサービス方法に関し、特に物流を伴うエレクトリックコマースに代表されるPKI（Public Key Infrastructure）サービスに関する。

【0002】

【従来の技術】近年、インタネットの普及に伴って、エレクトリックコマースに代表されるサービス、つまり通信販売等を代表とする物流を伴うサービスが普及してきている。このサービスは、主に商品の注文機能や代金の決済機能を電子的に支援するものである。

【0003】さらに、携帯電話やPDA（Personal Digital Assistants）等の携帯端末を用いたモバイルEC（Eletronic Commerce）も普及してきており、インタネットでのエレクトリックコマースにおいて、ネットワーク上の機能を提供するシステム（サービス）は多数存在する。

【0004】

【発明が解決しようとする課題】しかしながら、上述した従来のネットワーク上の機能を提供するシステムでは、インタネット上で商品を購入しても、実際には物流システムによってその商品が配送されているので、配達された商品が正当な送り主から送付されたのか、あるいは実際に注文した商品が送付されたのかを確認する作業を、商品を目で確認し、受領証に印鑑を捺印することで行わなければならず、配送時のトラブルが発生する恐れがある。

【0005】この場合、配送時のトラブルとしては商品の誤配、誰から送られてきたか分からないという差出人の不明、依頼品の確認を行うことができない等、宅配や一般の郵便（書留等）、通信販売、エレクトリックコマース等の物流部分における信頼性や安全性を確保することができないという問題がある。

【0006】したがって、従来のエレクトリックコマースでは、上述したような物流に伴う作業を電子的にサポートする機能を提供していないので、旧来の通信販売以上に普及していない。

【0007】そこで、本発明の目的は上記の問題点を解消し、物流部分における信頼性や安全性を向上させることができるロジスティックPKIサービスシステム、携帯端末及びそれに用いるロジスティックPKIサービス方法を提供することにある。

【0008】

【課題を解決するための手段】本発明によるロジスティックPKIサービスシステムは、配送物の配送時に当該配送物の情報を示すラベルデータを要求しかつ送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成する端末装置と、前記端末装置からの要求に応答して前記ラベルデータと前記配送物の認証情報とを発行する認証局と、配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行う携帯端末とを備えている。

【0009】本発明による携帯端末は、配送されてきた前記配送物に添付されているラベルから読取った情報と認証局からの当該配送物の認証情報とによって認証を行う手段を備えている。

【0010】本発明によるロジスティックPKIサービス方法は、端末装置において、配送物の配送時に当該配送物の情報を示すラベルデータを要求し、それに応答して送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成し、認証局において、前記端末装置からの要求に応答して前記ラベルデータと前記配送物の認証情報とを発行し、携帯端末において、配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行っている。

【0011】すなわち、本発明のロジスティックPKI（Public Key Infrastructure）サービスシステムは、店舗や郵便局等の端末装置が配送物の配送が依頼された時に当該配送物の情報を示すラベルデータを認証局に要求し、認証局がその要求に応答してラベルデータと当該配送物の認証情報とを発行し、店舗や郵便局等の端末装置が認証局からのラベルデータに基づいてラベルを生成して配送物に添付し、利用者の携帯端末が配送されてきた配送物に添付されているラベルから読取った情報と認証局からの認証情報とによって、利用者、配送物、店舗や郵便局等の認証を行うようにしている。

【0012】上記のように構成することで、本発明のロジスティックPKIサービスでは、誤配を防止したり、差出人の確認や依頼品の確認（通信販売のケース）を公開鍵の証明書を含む電子署名にて電子的に行うことが可能となり、贈答品等の宅配や一般の郵便（書留等）、通信販売、エレクトリックコマース（EC：Eletronic Commerce）の物流部分における信頼性や安全性を向上させることが可能となる。

【0013】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図1は本発明の第1の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。図1において、本発明の第1の実施例によるロジスティックPKIサービスシステムはPKI（Public Key Infrastructure）（認証局）1と、店舗端末2と、利用者の携帯端末4とから構成されている。尚、このシステムの物流部分には店舗から利用者への商品の配送等を行う物流業者3が介在する。

【0014】既存の物流を伴うサービスとしては、エレクトリックコマース（EC：Eletronic Commerce）（モバイルECを含む）、通信販売、贈答品等の一般の店舗での配送を伴う商品購入及びその宅配、一般の郵便（書留等）がある。本実施例ではモバイルECについて説明する。

【0015】モバイルECには、一般的に、取引がネットワーク上で行われる「リモート環境」と、実際に店舗での取引が存在する「ローカル環境」とがある。本実施例では「リモート環境」におけるロジスティックPKIサービスシステムを示している。

【0016】一般に、「リモート環境」とは、モバイルECにおいて、上記のように、取引のほとんどがネットワークを通じて行われる環境のことである。例えば、オンラインショッピングによる物品購入等がこれにあたる。

【0017】本実施例はモバイルECの物品販売等での物流に伴う認証サービス、つまりロジスティックPKIサービスを提供するものである。ロジスティックPKIサービスはこれまでの物流において発生していた問題、つまり配送や郵送される物品、依頼者、配送元が正しいものかどうかを証明するものの確認を行えないという問題を解決し、信頼性や安全性を向上、顧客の満足度を飛躍的に向上させる。また、ロジスティックPKIサービスは既存の物流システムに比較的容易に適合可能なため、導入が容易である。

【0018】このロジスティックPKIサービスはこれまでのエレクトリックコマースサービスでは解決されていない、商取引における物流に関わるサービスであり、顧客の満足度を飛躍的に向上させ、エレクトリックコマースの市場を確実に拡大させる。

【0019】ロジスティックPKIサービスでは、モバイルECにおいて、ネットワーク100上で購入した商品Bを配送する際に、認証局1が発行しかつ取引される商品Bに関する情報を物流ラベルAとして添付する。利用者が商品Bを物流業者3から受取る際に、その商品Bがどこから送られてきたのか、誰が注文したのか、商品Bは何なのか等の情報を電子的に証明する公開鍵の証明書を含む電子署名を、利用者の携帯端末4が物流ラベルAから読取り、それらを電子的に確認することが可能となる。

【0020】上述したサービスモデルは、ネットワーク100上での物品購入を想定した、いわゆるB2C（Business to Consumer）のモデルであり、利用者＝商品の受取り者、商品の送付者＝店舗、物流業者＝宅配業者である場合のモデルである。これ以外のモデルとして、同じB2Cでも、贈答品等のように利用者が注文者と受取り者とに分かれるモデル、一般郵便等のように店舗等が存在しないC2C（Consumer to Consumer）のモデルも考えられる。

【0021】いずれのモデルにおいても、利用者の携帯端末4、PKI（認証局）1、物流業者3の下でロジスティックPKIサービスを利用することで、安全な物流システムを提供することが可能となる。尚、本モデルは既存の通信販売に適用した場合にも、ほぼ同じサービスモデルであると考えられる。

【0022】図2は図1の利用者の携帯端末4の構成を示すブロック図である。図2において、利用者の携帯端末4はネットワーク100上で商品Bを注文するための商品注文機能41と、ネットワーク100上で購入した商品Bの配送を依頼するための配送依頼機能42と、電子署名を生成する署名生成機能43と、物流ラベルAを読取る物流ラベル読取り機能44と、読取った物流ラベルAの情報を復号する復号機能45と、復号された物流ラベルAの情報に基づいて認証を行う認証機能46とを含んで構成されている。

【0023】尚、利用者の携帯端末4の他の機能として考えられる携帯電話の電話機能や、PDA（Personal Digital Assistants）のデータ処理機能等については公知であるので、その構成や動作についての説明は省略する。また、商品注文機能41や配送依頼機能42には物流ラベルAを生成するための情報を発信する機能を持つ場合もある。

【0024】図3は図1のPKI1の構成を示すブロック図である。図3において、PKI1は店舗の公開鍵等の証明書を含む電子署名を発行する店舗証明書発行機能11と、利用者の公開鍵等の証明書を含む電子署名を発行する利用者証明書発行機能12と、店舗証明書発行機能11及び利用者証明書発行機能12で発行された電子署名と店舗端末2からの商品情報とを基に物流ラベルデータを発行する物流ラベルデータ発行機能13と、店舗証明書発行機能11及び利用者証明書発行機能12で発行される電子署名や物流ラベルデータ発行機能13で発行される物流ラベルデータを暗号化する暗号化機能14とを含んで構成されている。

【0025】図4は図1の店舗端末2の構成を示すブロック図である。図4において、店舗端末2にはPKI1に対する物流ラベルデータの発行要求やPKI1からの物流ラベルデータの処理を行う物流ラベルデータ処理機

能２１と、物流ラベルデータ処理機能２１で処理した物流ラベルデータを印刷する物流ラベルデータ印刷機能２２と、物流ラベルデータ印刷機能２２で印刷された物流ラベルＡを商品Ｂに添付する物流ラベル商品添付機能２３とからなる物流ラベル処理装置と、電子署名を生成する署名生成機能２４と、利用者の携帯端末４との間の通信を行う携帯端末間通信機能２５とを含んで構成されている。

【００２６】物流ラベルデータ処理機能２１はネットワーク１００を介してＰＫＩ１からディジタルデータとして送付されてくる物流ラベルデータを処理し、物流ラベルデータ印刷機能２２は物流ラベルデータ処理機能２１で処理された物流ラベルデータを物流ラベルＡとして印刷する。物流ラベル商品添付機能２３は物流ラベルデータ印刷機能２２で印刷された物流ラベルＡを商品Ｂに添付する。

【００２７】尚、物流ラベル処理装置は店舗に置く場合、店舗の物流業者として一般の宅配業者が採用されていれば、その宅配受付窓口の数だけ設置する。また、物流ラベル処理装置は物流業者３に設置することも可能である。

【００２８】図５は本発明の第１の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。これら図１～図５を参照して本発明の第１の実施例によるロジスティックＰＫＩサービスシステムの動作について説明する。尚、以下の説明では、利用者、店舗がそれぞれ秘密鍵を持ち、ＰＫＩ１がそれらの秘密鍵に対する公開鍵を認証する公開鍵証明書を電子署名として発行するものとする。

【００２９】まず、利用者が携帯端末４の商品注文機能４１や配送依頼機能４２からネットワーク１００を介して、店舗端末２に掲示された商品Ｂの購入や当該商品Ｂの配送依頼を行うと（図１のａ）（図５ステップＳ１）、店舗端末２は物流ラベルデータ処理機能２１を用いて利用者の携帯端末４から入力される情報（利用者公開鍵・商品情報・商品情報への利用者秘密鍵による署名）を基にＰＫＩ１に物流ラベルデータの発行を要求する（図１のｂ）（図５ステップＳ２）。

【００３０】ＰＫＩ１はその物流ラベルデータの発行要求に応答して、店舗端末２から入力される情報（利用者公開鍵・商品情報・店舗公開鍵・商品情報への利用者秘密鍵による署名・注文ＩＤ・注文ＩＤへの店舗秘密鍵による署名）を基に店舗証明書発行機能１１にて店舗の公開鍵証明書を発行し（図５ステップＳ３）、物流ラベルデータ発行機能１３にて商品情報への署名・注文ＩＤへの署名を利用者の公開鍵で暗号化して物流ラベルデータを作成する（図５ステップＳ４）。

【００３１】ＰＫＩ１は作成した物流ラベルデータを店舗端末２に送信するとともに（図１のｃ）（図５ステップＳ５）、上記の情報（商品情報・注文ＩＤ・店舗の公開鍵証明書）を暗号化機能１４にて利用者の公開鍵を基に暗号化した認証情報を、利用者の携帯端末４に電子メール等を用いて送信する（図１のｄ）（図５ステップＳ６）。

【００３２】店舗端末２はＰＫＩ１から発行される物流ラベルデータを受取ると、ＰＫＩ１からの物流ラベルデータに基づいて物流ラベルＡを生成し、その物流ラベルＡを商品Ｂに添付した後（図１のｅ）（図５ステップＳ７）、商品Ｂの配送依頼を物流業者３に依頼する（図１のｆ）。

【００３３】ここで、物流ラベルＡとは店舗ＩＤ（店舗の公開鍵証明書そのものか、それから得られるＩＤ等）と、商品情報と、利用者ＩＤ（利用者の公開鍵証明書そのものか、それから得られるＩＤ等）または利用者が生成した電子署名とを利用者の公開鍵で暗号化した情報から生成された二次元バーコード、あるいはその情報を格納するＩＣタグ等である。また、上述した公開鍵や公開鍵証明書の送信は全て、公開鍵や公開鍵証明書から得られるＩＤの送信に置き換えることができる。

【００３４】利用者の携帯端末４はＰＫＩ１から送信される認証情報を受信し、物流業者３によって商品Ｂが配送されると（図１のｇ）（図５ステップＳ８）、物流ラベル読取り機能４４にて商品Ｂに添付された物流ラベルＡの情報を読取る（図５ステップＳ９）。

【００３５】この場合、物流ラベル読取り機能４４は物流ラベルＡが二次元バーコードであれば、その二次元バーコードを読取るためのスキャナ機能か、物流業者の使用している端末のスキャナ機能にて二次元バーコードを読取った情報を受取るためのインタフェースかを備え、物流ラベルＡがＩＣタグであれば、ＩＣタグから情報を読取る機能を備えている。

【００３６】利用者の携帯端末４は物流ラベル読取り機能４４で読取った物流ラベルＡの情報を復号機能４５にて利用者の秘密鍵を基に復号し（図５ステップＳ１０）、認証機能４６にて物流ラベルＡの情報とＰＫＩ１からの認証情報とによる認証を行う（図１のｈ）（図５ステップＳ１１）。

【００３７】ここで、認証機能４６は物流ラベルＡの情報とＰＫＩ１からの認証情報とを比較することで、物流ラベルＡと認証情報とから得られる商品情報・注文ＩＤ・店舗の公開鍵証明書をそれぞれ検証、確認するとともに、その検証、確認の結果を図示せぬ画面上に表示する。

【００３８】これによって、利用者はその商品Ｂがどこから送られてきたのか、誰が注文したのか、商品Ｂは何なのか等の情報を、電子的に証明する公開鍵の証明書を含む電子署名にて電子的に確認することができる。

【００３９】図６は本発明の第２の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。図６において、本発明の第２の実施例による

ロジスティックＰＫＩサービスシステムは店舗での配送を伴う商品購入でのローカル環境のサービスモデルを示している。

【００４０】尚、本発明の第２の実施例によるロジスティックＰＫＩサービスシステムは店舗において配送を伴う商品購入を行う以外は図１に示す本発明の第１の実施例によるロジスティックＰＫＩサービスシステムと同様の動作である。この場合、申込者及び受取者はネットワーク１００を介することなく、上記の利用者の携帯端末４を用いて商品Ｂの購入申込み及び受取りを行う点以外は本発明の第１の実施例によるロジスティックＰＫＩサービスシステムと同様である。

【００４１】一般に、ローカル環境とはモバイルＥＣにおいて、取引の一部が実際の店舗で行われる環境であり、例えば、モバイルを決済等に利用したコンビニエンスストアでの物品購入等がある。

【００４２】ロジスティックＰＫＩサービスでは、店舗での配送を伴う商品購入において、店舗で購入した商品Ｂを配送する際に、ＰＫＩ１が発行しかつ取引される商品Ｂに関する情報を物流ラベルＡとして添付する。受取者が商品Ｂを物流業者３から受取る際に、その商品Ｂがどこから送られてきたのか、誰が注文したのか、商品Ｂは何なのか等を電子的に証明する公開鍵の証明書を含む電子署名を携帯端末４によって物流ラベルＡから読取り、それらを電子的に確認することが可能となる。

【００４３】上述したサービスモデルは、店舗での物品購入を想定した、いわゆるＢ２Ｃのモデルであり、申込者＝商品の購入者、受取者＝商品の受取者、商品の送付者＝店舗、物流業者＝宅配業者である場合のモデルであり、申込者及び受取者の携帯端末４、ＰＫＩ（認証局）１、物流業者３の下でロジスティックＰＫＩサービスを利用することで、安全な物流システムを提供することが可能となる。尚、宅配やＰ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ）である一般の郵便（書留等）に適用した場合にもほぼ同じサービスモデルとなる。

【００４４】本実施例において用いられる携帯端末４（申込者の携帯端末４ａ及び受取者の携帯端末４ｂ）の構成は図２に示す本発明の第１の実施例の携帯端末４と同様の構成となっている。申込者の携帯端末４ａでは配送依頼機能４２を用いて店舗内のＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅｓ）（図示せず）との間で通信を行い、店舗で購入した商品Ｂの配送を依頼する。

【００４５】本実施例では店舗内のＰＯＳが店舗端末２に相当し、配送依頼機能４２は店舗端末２の携帯端末間通信機能２５との間で通信を行うこととなる。これら配送依頼機能４２と携帯端末間通信機能２５との間での通信としては、非接触ＩＣ（集積回路）、ＩｒＤＡ（Ｉｎｆｒａｒｅｄ　Ｄａｔａ　Ａｓｓｏｃｉａｔｉｏｎ）、Ｂｌｕｅｔｏｏｔｈ（Ｒ）等が考えられ、物流ラベルＡを生成するための情報を発信する場合もある。

【００４６】一方、受取者の携帯端末４ｂでは物流ラベル読取り機能４４が物流ラベルＡの情報を読取り、復号機能４５が読取った物流ラベルＡの情報を受取者の秘密鍵を用いて復号し、認証機能４６が復号機能４５で復号された物流ラベルＡの情報に基づいて認証を行う。尚、申込者の携帯端末４ａ及び受取者の携帯端末４ｂの他の機能としては、図２に示す本発明の第１の実施例の携帯端末４と同様に、携帯電話の電話機能や、ＰＤＡのデータ処理機能等がある。

【００４７】本実施例において用いられるＰＫＩ１の構成は図３に示す本発明の第１の実施例のＰＫＩ１と同様の構成となっている。このＰＫＩ１においては利用者証明書発行機能１２による利用者の証明書が上記の携帯端末４の数（＋α）だけ必要となり、物流ラベルデータ発行機能１３による物流ラベルデータの発行は物流トランザクション毎に発生することとなる。

【００４８】本実施例において用いられる店舗端末２の物流ラベル処理装置の構成は図４に示す本発明の第１の実施例の店舗端末２と同様の構成となっている。物流ラベルデータの発行は上述したＰＫＩ１で行われるが、実際の商品Ｂへ物流ラベルＡを添付するのは店舗または物流業者の物流ラベル処理装置で行われ、そのための装置が必要となる。

【００４９】図７は本発明の第２の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。これら図２～図４と図６と図７とを参照して本発明の第２の実施例によるロジスティックＰＫＩサービスシステムの動作について説明する。尚、以下の説明では、申込者、受取者、店舗がそれぞれ秘密鍵を持ち、ＰＫＩ１がそれらの秘密鍵に対する公開鍵を認証する公開鍵証明書を電子署名として発行するものとする。

【００５０】まず、申込者が携帯端末４ａの配送依頼機能４２から店舗端末２の携帯端末間通信機能２５を介して商品Ｂの配送依頼を行うと（図６のａ）（図７ステップＳ２１）、店舗端末２は物流ラベルデータ処理機能２１を用いて利用者の携帯端末４から入力される情報（申込者公開鍵・受取者公開鍵・商品情報・商品情報への申込者秘密鍵による署名）を基にＰＫＩ１に物流ラベルデータの発行を要求する（図６のｂ）（図７ステップＳ２２）。

【００５１】ＰＫＩ１はその物流ラベルデータの発行要求に応答して、店舗端末２から入力される情報（申込者公開鍵・受取者公開鍵・商品情報・商品情報への申込者秘密鍵による署名・店舗公開鍵・注文ＩＤ・注文ＩＤへの店舗秘密鍵による署名）を基に店舗証明書発行機能１１と利用者証明書発行機能１２とを用いて申込者、店舗それぞれの公開鍵証明書を発行し（図７ステップＳ２３）、物流ラベルデータ発行機能１３にて商品情報への署名・注文ＩＤへの署名を受取者の公開鍵で暗号化して

物流ラベルデータを作成する（図7ステップＳ２４）。
【００５２】ＰＫＩ１は作成した物流ラベルデータを店舗端末２に送信するとともに（図６のｃ）（図７ステップＳ２５）、上記の情報（商品情報・注文ＩＤ・申込者の公開鍵証明書・店舗の公開鍵証明書）を暗号化機能１４にて受取者の公開鍵を基に暗号化した認証情報を、受取者の携帯端末４ｂに電子メール等を用いて送信する（図６のｄ）（図７ステップＳ２６）。
【００５３】店舗端末２はＰＫＩ１から発行される物流ラベルデータを受取ると、ＰＫＩ１からの物流ラベルデータに基づいて物流ラベルＡを生成し、その物流ラベルＡを商品Ｂに添付した後（図６のｅ）（図７ステップＳ２７）、商品Ｂの配送依頼を物流業者３に依頼する（図６のｆ）（図７ステップＳ２８）。
【００５４】ここで、物流ラベルＡとは店舗ＩＤ（店舗の公開鍵証明書そのものか、それから得られるＩＤ等）と、商品情報と、申込者ＩＤ（申込者の公開鍵証明書そのものか、それから得られるＩＤ等）または申込者が生成した電子署名とを受取者の公開鍵で暗号化した情報から生成された二次元バーコード、あるいはその情報を格納するＩＣタグ等である。また、上述した公開鍵や公開鍵証明書の送信は全て、公開鍵や公開鍵証明書から得られるＩＤの送信に置き換えることができる。
【００５５】受取者の携帯端末４ｂはＰＫＩ１から送信される認証情報を受信し、物流業者３によって商品Ｂが配送されると（図６のｇ）（図７ステップＳ２９）、物流ラベル読取り機能４４にて商品Ｂに添付された物流ラベルＡの情報を読取る（図７ステップＳ３０）。
【００５６】この場合、物流ラベル読取り機能４４は物流ラベルＡが二次元バーコードであれば、その二次元バーコードを読取るためのスキャナ機能か、物流業者の使用している端末のスキャナ機能にて二次元バーコードを読取った情報を受取るためのインタフェースかを備え、物流ラベルＡがＩＣタグであれば、ＩＣタグから情報を読取る機能を備えている。
【００５７】受取者の携帯端末４ｂは物流ラベル読取り機能４４で読取った物流ラベルＡの情報を復号機能４５にて受取者の秘密鍵を基に復号し（図７ステップＳ３１）、認証機能４６にて物流ラベルＡの情報とＰＫＩ１からの認証情報とによる認証を行う（図６のｈ）（図７ステップＳ３２）。
【００５８】ここで、認証機能４６は物流ラベルＡの情報とＰＫＩ１からの認証情報とを比較することで、物流ラベルＡと認証情報とから得られる商品情報・注文ＩＤ・申込者の公開鍵証明書・店舗の公開鍵証明書をそれぞれ検証、確認するとともに、その検証、確認の結果を図示せぬ画面上に表示する。
【００５９】これによって、受取者はその商品Ｂがどこから送られてきたのか、誰が注文したのか、商品Ｂは何なのか等の情報を、電子的に証明する公開鍵の証明書を含む電子署名にて電子的に確認することができる。
【００６０】図８は本発明の第３の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。図８において、本発明の第３の実施例によるロジスティックＰＫＩサービスシステムは店舗での配送を伴う商品購入でのローカル環境のサービスモデルを示している。
【００６１】尚、本発明の第３の実施例によるロジスティックＰＫＩサービスシステムは申込者が携帯端末４ａにてネットワーク１００を介して店舗から商品購入を行う以外は図６に示す本発明の第２の実施例によるロジスティックＰＫＩサービスシステムと同様の動作である。
【００６２】図９は本発明の第４の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。図９において、本発明の第４の実施例によるロジスティックＰＫＩサービスシステムは店舗での配送を伴う商品購入でのローカル環境のサービスモデルを示している。
【００６３】尚、本発明の第４の実施例によるロジスティックＰＫＩサービスシステムは受取者が電子的に確認した内容を申込者にネットワーク１００を介して通知するように以外は図６に示す本発明の第２の実施例によるロジスティックＰＫＩサービスシステムと同様の動作である。
【００６４】図１０は本発明の第４の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。図１０において、ステップＳ２１～Ｓ３２は図７に示す本発明の第２の実施例によるロジスティックＰＫＩサービスシステムの動作と同様であるので、その説明は省略する。
【００６５】受取者の携帯端末４ｂは認証機能４６による物流ラベルＡの情報とＰＫＩ１からの認証情報とによる認証結果を申込者の携帯端末４ａにネットワーク１００を介して通知する（図９のｉ）（図１０ステップＳ３３）。この場合、受取者の携帯端末４ｂは復号機能４５にて復号された物流ラベルＡの情報と商品Ｂの受取り情報とを電子メール等で申込者の携帯端末４ａに通知する。
【００６６】よって、申込者は配送依頼を行った商品Ｂを受取者が受取ったことを電子的に確認することができる。尚、上述した本発明の第１～第４の実施例における物流ラベルＡを用いることで、物流業者３による商品Ｂの配送状況をネットワーク１００上で確認することも可能である。
【００６７】図１１は本発明の第５の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。図１１において、本発明の第５の実施例によるロジスティックＰＫＩサービスシステムは郵便（書留等）に適用した場合のサービスモデルを示しており、ＰＫＩ（認証局）１と、郵便局端末５と、申込者の携帯

端末６ａ及び受取者の携帯端末６ｂとから構成されている。

【００６８】上述した本発明の第１の実施例及び第２の実施例は、利用者が商品を店舗で購入して物流が発生するという点で、すべてＢ２Ｃである。しかしながら、本実施例による既存の郵便（書留等）への適用は、郵便という物流は伴うものの、商品自身が基本的に送り主、受取り主の所有物である点で、Ｐ２Ｐである。

【００６９】ロジスティックＰＫＩサービスでは、郵便物Ｄの郵送において、郵便局で依頼した郵便物Ｄを郵送する際に、ＰＫＩ１が発行する郵送される郵便物Ｄに関する情報を郵便ラベルＣとして添付する。受取者が郵便物Ｄを郵便事業者から受取る際に、その郵便物Ｄがどこから送られてきたのか、誰が郵送を依頼したのか等を、携帯端末６ｂによって郵便ラベルＣから読取り、電子的に確認することが可能となる。

【００７０】上述したサービスモデルは、郵便局を介した郵便物Ｄの郵送を想定した、いわゆるＰ２Ｐのモデルであり、申込者＝郵便物の郵送依頼者、受取者＝郵便物の受取者、郵便物の郵送者＝郵便事業者のモデルであり、申込者の携帯端末６ａ及び受取者の携帯端末６ｂ、ＰＫＩ１、郵便事業者の下でロジスティックＰＫＩを利用することによって、安全な郵便システムを提供することが可能となる。尚、個人の依頼する宅配に適用した場合にも、ほぼ同じサービスモデルとなる。

【００７１】図１２は図１１の携帯端末６ａ，６ｂの構成を示すブロック図である。図7において、携帯端末６は郵便物の郵送を依頼する郵送依頼機能６１と、電子署名を生成する署名生成機能４３と、郵便ラベルＣを読取る郵便ラベル読取り機能６２と、読取った郵便ラベルＣの情報を復号する復号機能４５と、復号された郵便ラベルＣの情報に基づいて認証を行う認証機能４６とを含んで構成されている。申込者の携帯端末６ａ及び受取者の携帯端末６ｂは上記の携帯端末６と同様の構成及び動作となっている。

【００７２】尚、申込者の携帯端末６ａ及び受取者の携帯端末６ｂの他の機能として考えられる携帯電話の電話機能や、ＰＤＡのデータ処理機能等については公知であるので、その構成や動作についての説明は省略する。

【００７３】また、郵送依頼機能６１は郵便局内のＰＯＳ（図示せず）との間で通信を行い、郵便物Ｄの郵送を依頼する。この郵送依頼機能６１としては非接触ＩＣ、ＩｒＤＡ、Ｂｌｕｅｔｏｏｔｈ（Ｒ）等が考えられ、郵便ラベルＣを生成するための情報を発信する場合もある。

【００７４】図１３は図１１のＰＫＩ１の構成を示すブロック図である。図１３において、ＰＫＩ１は郵便局の公開鍵等の証明書を含む電子署名を発行する郵便局証明書発行機能１５と、申込者及び受取者の公開鍵等の証明書を含む電子署名を発行する利用者証明書発行機能１２と、郵便局証明書発行機能１５及び利用者証明書発行機能１２で発行された電子署名と郵便局舗端末５からの郵便物情報とを基に郵便ラベルデータを発行する郵便ラベルデータ発行機能１６と、郵便局証明書発行機能１５及び利用者証明書発行機能１２で発行される電子署名や郵便ラベルデータ発行機能１６で発行される郵便ラベルデータを暗号化する暗号化機能１４とを含んで構成されている。

【００７５】このＰＫＩ１においては利用者証明書発行機能１２による申込者及び受取者の証明書が上記の携帯端末６の数（＋α）だけ必要となり、郵便ラベルデータ発行機能１６による郵便ラベルデータの発行は郵便トランザクション毎に発生することとなる。

【００７６】図１４は図１１の郵便局端末５の構成を示すブロック図である。図１４において、郵便局端末５にはＰＫＩ１に対する郵便ラベルデータの発行要求やＰＫＩ１からの郵便ラベルデータの処理を行う郵便ラベルデータ処理機能５１と、郵便ラベルデータ処理機能５１で処理した郵便ラベルデータを印刷する郵便ラベルデータ印刷機能５２と、郵便ラベルデータ印刷機能５２で印刷された郵便ラベルＣを郵便物Ｄに添付する郵便ラベル郵便物添付機能５３とからなる郵便ラベル処理装置と、電子署名を生成する署名生成機能５４と、申込者の携帯端末６ａとの間の通信を行う携帯端末間通信機能５５とを含んで構成されている。郵便ラベルデータの発行は上述したＰＫＩ１で行われるが、実際の郵便物Ｄへ郵便ラベルＣを添付するのは郵便局の郵便ラベル処理装置で行われる。

【００７７】郵便ラベルデータ処理機能５１はネットワーク１００を介してＰＫＩ１からディジタルデータとして送付されてくる郵便ラベルデータを処理し、郵便ラベルデータ印刷機能５２は郵便ラベルデータ処理機能５１で処理された郵便ラベルデータを郵便ラベルＣとして印刷する。郵便ラベル郵便物添付機能５３は郵便ラベルデータ印刷機能５２で印刷された郵便ラベルＣを郵便物Ｄに添付する。

【００７８】図１５は本発明の第５の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。これら図１１～図１５を参照して本発明の第５の実施例によるロジスティックＰＫＩサービスシステムの動作について説明する。尚、以下の説明では、申込者、受取者、郵便局がそれぞれ秘密鍵を持ち、ＰＫＩ１がそれらの秘密鍵に対する公開鍵を認証する公開鍵証明書を電子署名として発行するものとする。

【００７９】まず、申込者は携帯端末６ａを用いて郵便物Ｄの郵送依頼を行うと（図１１のａ）（図１５ステップＳ４１）、郵便局端末５は郵便ラベルデータ処理機能５１を用いて申込者の携帯端末６ａから入力される情報（申込者公開鍵・受取者公開鍵・郵便物情報・郵便物情報への申込者秘密鍵による署名）を基にＰＫＩ１に郵便

ラベルデータの発行を要求する（図１１のｂ）（図１５ステップＳ４２）。

【００８０】ＰＫＩ１はその郵便ラベルデータの発行要求に応答して、郵便局端末５から入力される情報（申込者公開鍵・受取者公開鍵・郵便物情報・郵便物情報への申込者秘密鍵による署名・郵便局公開鍵・郵便ＩＤ・郵便ＩＤへの郵便局秘密鍵による署名）を基に郵便局証明書発行機能１５と利用者証明書発行機能１２とを用いて申込者、郵便局それぞれの公開鍵証明書を発行し（図１５ステップＳ４３）、郵便ラベルデータ発行機能１６にて郵便物情報への署名・郵便ＩＤへの署名を受取者の公開鍵で暗号化して郵便ラベルデータを作成する（図１５ステップＳ４４）。

【００８１】ＰＫＩ１は作成した郵便ラベルデータを郵便局端末５に送信するとともに（図１１のｃ）（図１５ステップＳ４５）、上記の情報（郵便物情報・郵便ＩＤ・申込者の公開鍵証明書・郵便局の公開鍵証明書）を暗号化機能１４にて受取者の公開鍵を基に暗号化し、受取者の携帯端末６ｂに電子メール等を用いて送信する（図１１のｄ）（図１５ステップＳ４６）。

【００８２】郵便局端末５はＰＫＩ１から発行される郵便ラベルデータを受取ると、ＰＫＩ１からの郵便ラベルデータに基づいて郵便ラベルＣを生成し、その郵便ラベルＣを郵便物Ｄに添付した後（図１１のｅ）（図１５ステップＳ４７）、郵便物Ｄの郵送を行う（図１１のｆ）（図１５ステップＳ４８）。

【００８３】ここで、郵便ラベルＣとは郵便局ＩＤ（郵便局の公開鍵証明書そのものか、それから得られるＩＤ等）と、郵便物情報と、申込者ＩＤ（申込者の公開鍵証明書そのものか、それから得られるＩＤ等）または申込者が生成した電子署名とを受取者の公開鍵で暗号化した情報から生成された二次元バーコード、あるいはその情報を格納するＩＣタグ等である。また、上述した公開鍵や公開鍵証明書の送信は全て、公開鍵や公開鍵証明書から得られるＩＤの送信に置き換えることができる。

【００８４】受取者の携帯端末６ｂはＰＫＩ１から送信される認証情報を受信し、郵便局から郵便物Ｄが郵送されると、郵便ラベル読取り機能６２にて郵便物Ｄに添付された郵便ラベルＣの情報を読取る（図１５ステップＳ４９）。

【００８５】この場合、郵便ラベル読取り機能６２は郵便ラベルＣが二次元バーコードであれば、その二次元バーコードを読取るためのスキャナ機能か、郵便局員の使用している端末のスキャナ機能にて二次元バーコードを読取った情報を受取るためのインタフェースかを備え、郵便ラベルＣがＩＣタグであれば、ＩＣタグから情報を読取る機能を備えている。

【００８６】受取者の携帯端末６ｂは郵便ラベル読取り機能６２で読取った郵便ラベルＣの情報を復号機能４５にて受取者の秘密鍵を基に復号し（図１５ステップＳ５０）、認証機能４６にて郵便ラベルＣの情報とＰＫＩ１からの認証情報とによる認証を行う（図１１のｈ）（図１５ステップＳ５１）。

【００８７】ここで、認証機能４６は郵便ラベルＣの情報とＰＫＩ１からの認証情報とを比較することで、郵便ラベルＣと認証情報とから得られる郵便物情報・郵便ＩＤ・申込者の公開鍵証明書・郵便局の公開鍵証明書をそれぞれ検証、確認するとともに、その検証、確認の結果を図示せぬ画面上に表示する。

【００８８】これによって、受取者はその郵便物Ｄが誰から送られてきたのか、郵便物Ｄは何なのか等の情報を、電子的に証明する公開鍵の証明書を含む電子署名にて電子的に確認することができる。

【００８９】

【発明の効果】以上説明したように本発明は、認証局が、配送物の配送が依頼された時に当該配送物の情報を示すラベルデータと当該配送物の認証情報とを発行し、端末装置が、認証局からのラベルデータに基づいてラベルを生成して配送物に添付し、携帯端末が、配送されてきた配送物に添付されているラベルから読取った情報と認証局からの認証情報とによって認証を行うことによって、物流部分における信頼性や安全性を向上させることができるという効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。

【図２】図１の利用者携帯端末の構成を示すブロック図である。

【図３】図１のＰＫＩの構成を示すブロック図である。

【図４】図１の店舗端末の構成を示すブロック図である。

【図５】本発明の第１の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。

【図６】本発明の第２の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。

【図７】本発明の第２の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。

【図８】本発明の第３の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。

【図９】本発明の第４の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。

【図１０】本発明の第４の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。

【図１１】本発明の第５の実施例によるロジスティックＰＫＩサービスシステムの構成を示すブロック図である。

【図１２】図１１の携帯端末の構成を示すブロック図で

ある。

【図１３】図１１のＰＫＩの構成を示すブロック図である。

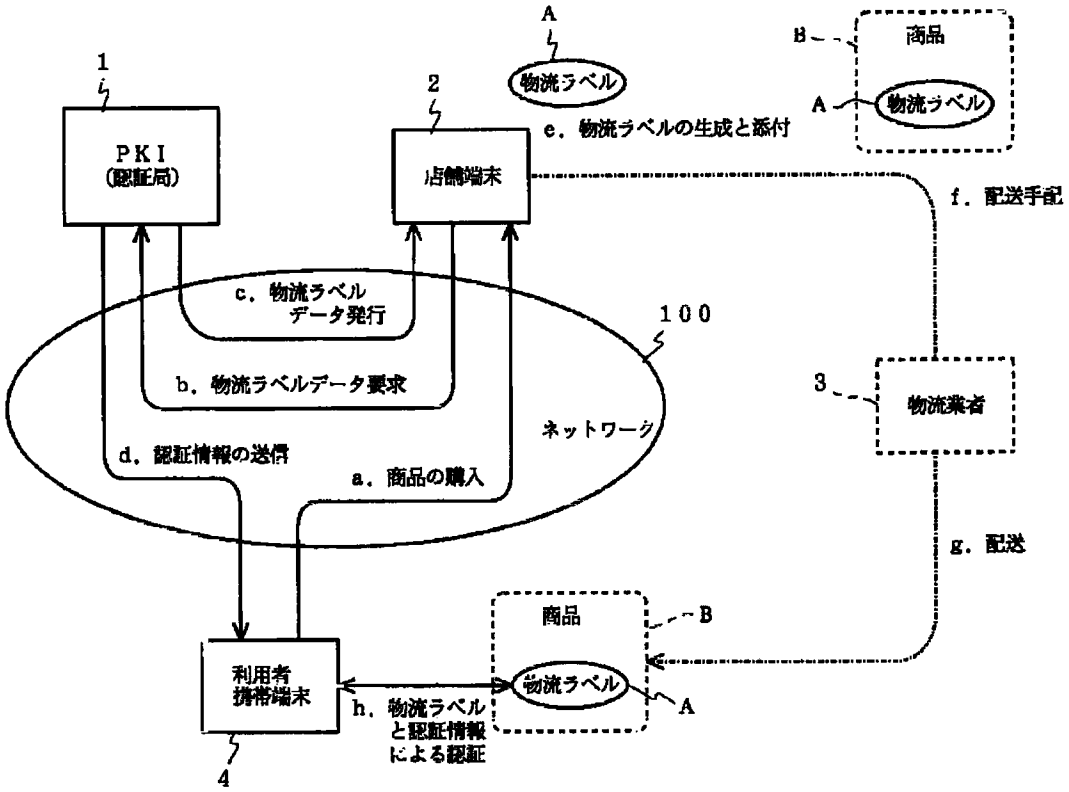
【図１４】図１１の郵便局端末の構成を示すブロック図である。

【図１５】本発明の第５の実施例によるロジスティックＰＫＩサービスシステムの動作を示すシーケンスチャートである。

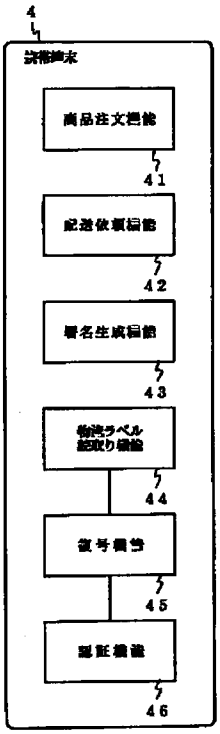
【符号の説明】

１　ＰＫＩ
２　店舗端末
３　物流業者
４，４ａ，４ｂ，
６，６ａ，６ｂ　携帯端末
５　郵便局端末
１１　店舗証明書発行機能
１２　利用者証明書発行機能
１３　物流ラベルデータ発行機能
１４　暗号化機能
１５　郵便局証明書発行機能
１６　郵便ラベルデータ発行機能
２１　物流ラベルデータ処理機能
２２　物流ラベルデータ印刷機能
２３　物流ラベル商品添付機能
２４，４３，５４　署名生成機能
２５，５５　携帯端末間通信機能
４１　商品注文機能
４２　配送依頼機能
４４　物流ラベル読取り機能
４５　復号機能
４６　認証機能
５１　郵便ラベルデータ処理機能
５２　郵便ラベルデータ印刷機能
５３　郵便ラベル郵便物添付機能
６１　郵送依頼機能
６２　郵便ラベル読取り機能
１００　ネットワーク
Ａ　物流ラベル
Ｂ　商品
Ｃ　郵便ラベル
Ｄ　郵便物

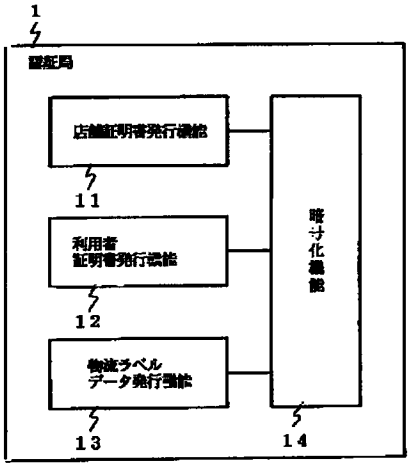
【図１】



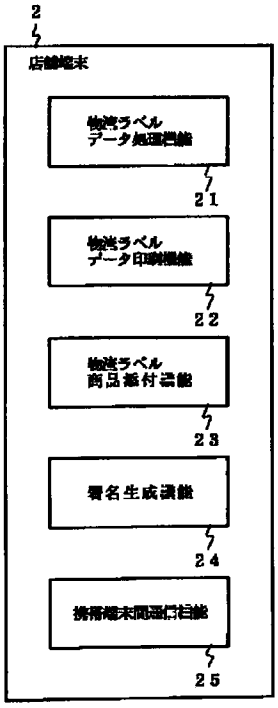
【図2】



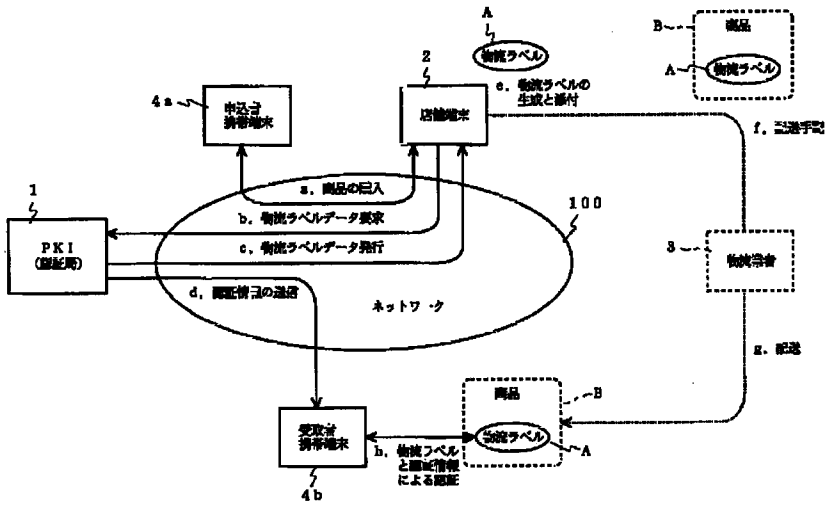
【図3】



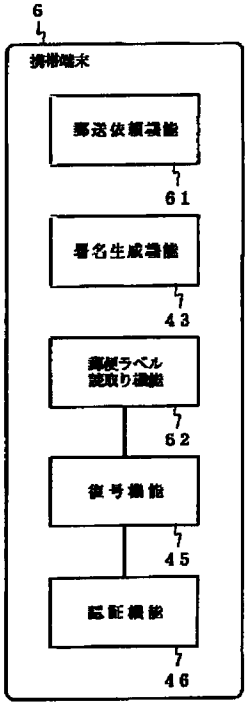
【図4】



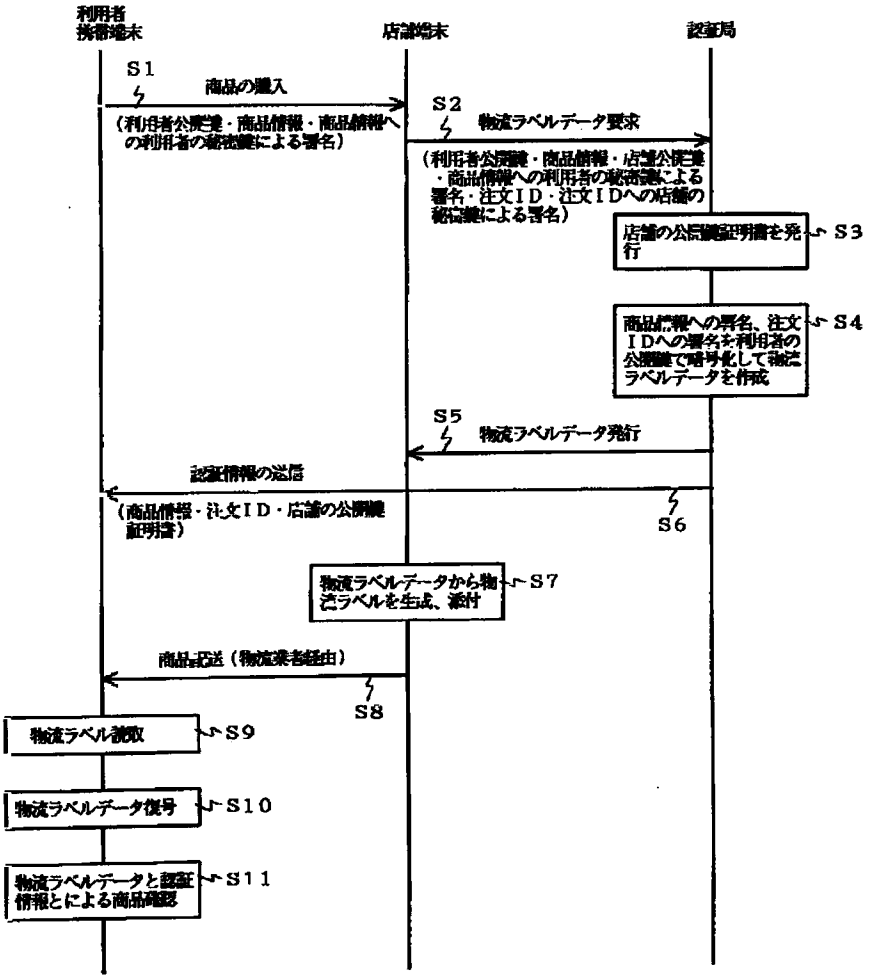
【図8】



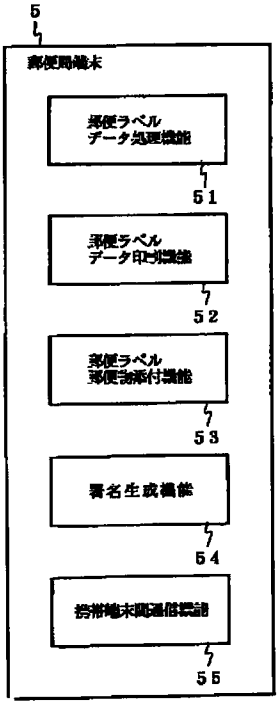
【図12】



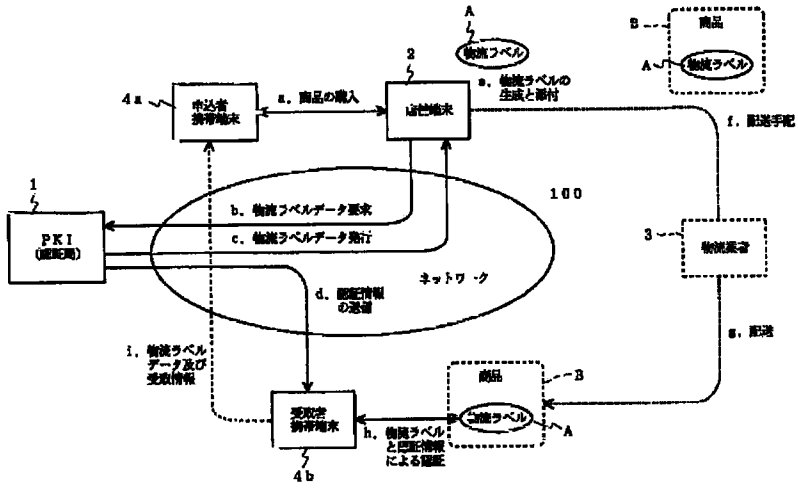
【図5】


利用者
携帯端末
店舗端末
認証局
S1
商品の購入
(利用者公開鍵・商品情報・商品情報への利用者の秘密鍵による署名)
S2
物流ラベルデータ要求
(利用者公開鍵・商品情報・店舗公開鍵・商品情報への利用者の秘密鍵による署名・注文ID・注文IDへの店舗の秘密鍵による署名)
店舗の公開鍵証明書を発行
S3
商品情報への署名、注文IDへの署名を利用者の公開鍵で暗号化して物流ラベルデータを作成
S4
S5
物流ラベルデータ発行
認証情報の送信
(商品情報・注文ID・店舗の公開鍵証明書)
S6
物流ラベルデータから物流ラベルを生成、添付
S7
商品の配送(物流業者経由)
S8
物流ラベル読取
S9
物流ラベルデータ復号
S10
物流ラベルデータと認証情報とによる商品確認
S11

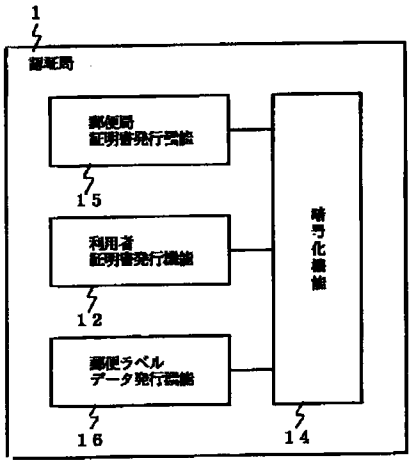
【図14】


5
郵便局端末
郵便ラベルデータ処理機能
51
郵便ラベルデータ印刷機能
52
郵便ラベル郵便番号付機能
53
署名生成機能
54
携帯端末間通信機能
55

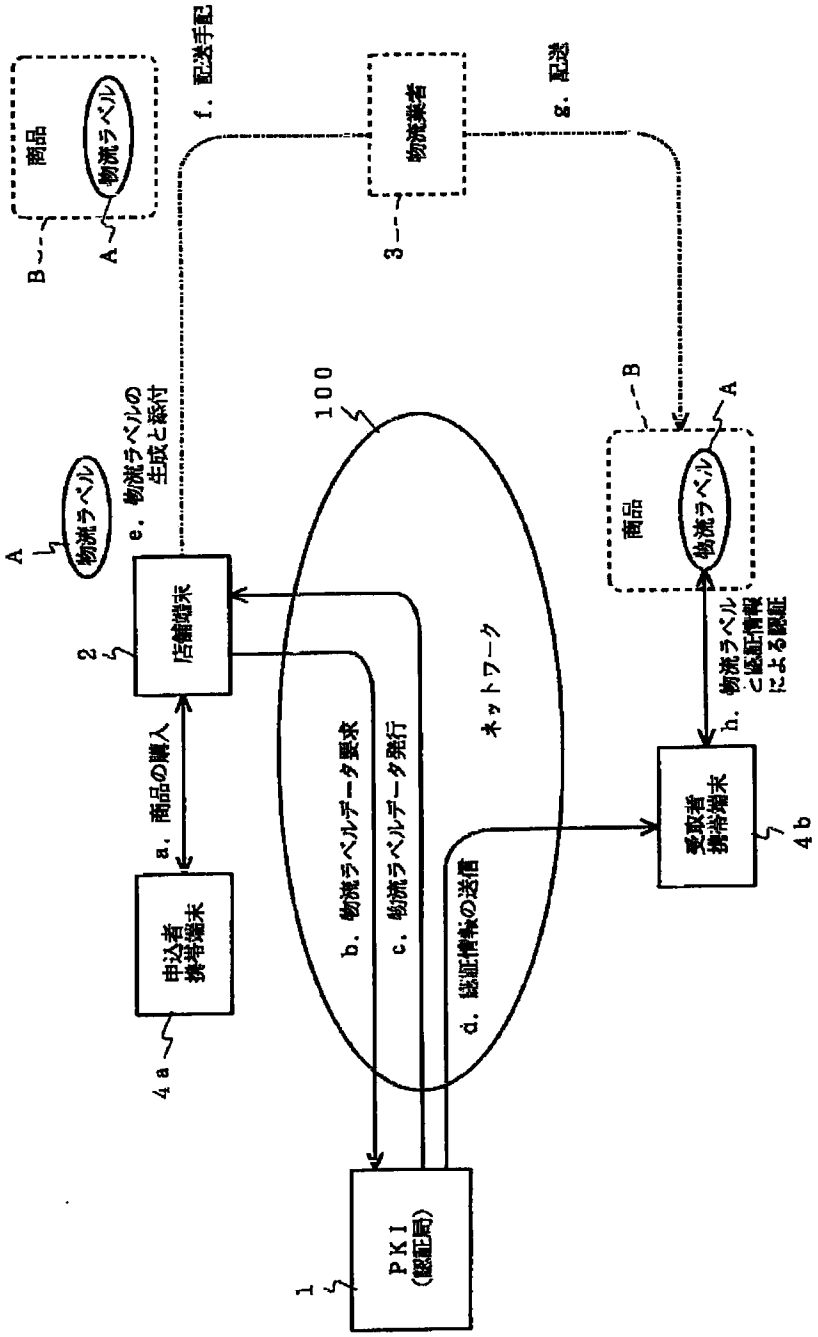
【図9】


A
物流ラベル
B
商品
2
a. 物流ラベルの生成と添付
4a
申込者携帯端末
a. 商品の購入
店舗端末
f. 配送手配
1
PKI(認証局)
100
b. 物流ラベルデータ要求
c. 物流ラベルデータ発行
ネットワーク
3
物流業者
d. 認証情報の送信
g. 配送
i. 物流ラベルデータ及び受取情報
受取者携帯端末
h. 物流ラベルと認証情報による認証
4b

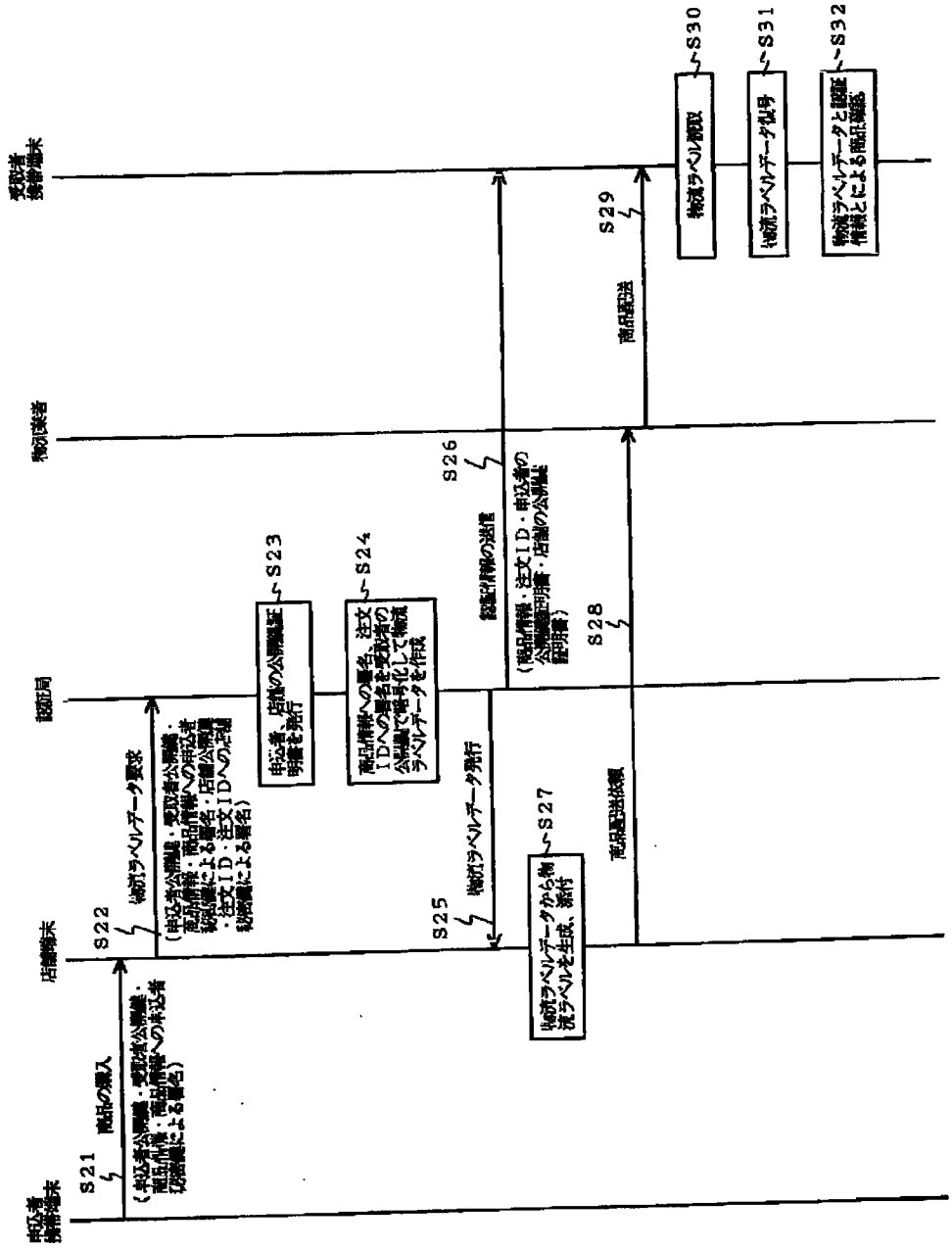
【図13】


1
認証局
郵便局証明書発行機能
15
利用者証明書発行機能
12
郵便ラベルデータ発行機能
16
暗号化機能
14

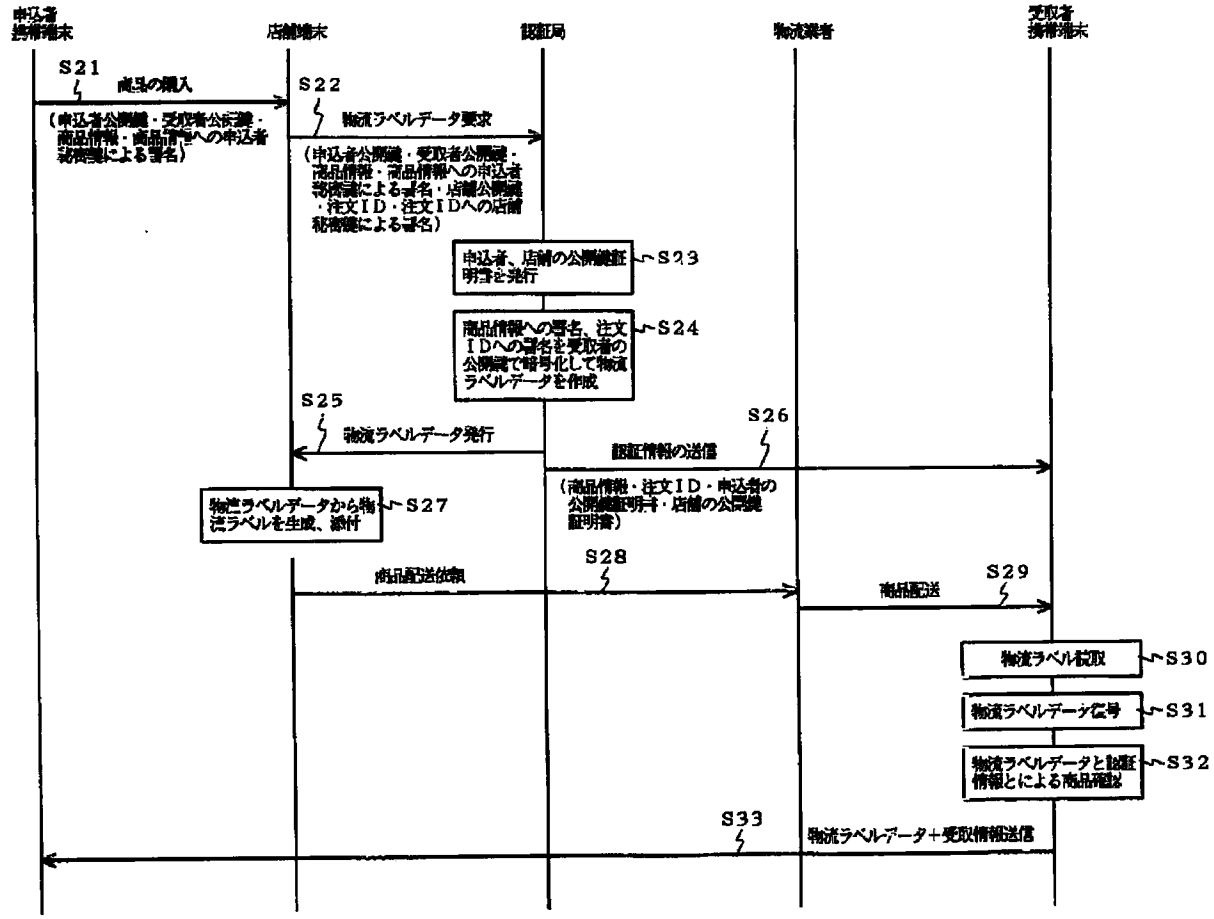
【図6】


商品
物流ラベル
B
A
f．配送手配
物流業者
3
g．配送
100
e．物流ラベルの生成と添付
A
物流ラベル
店舗端末
2
a．商品の購入
申込者携帯端末
4a
b．物流ラベルデータ要求
c．物流ラベルデータ発行
d．認証情報の送信
ネットワーク
PKI（認証局）
1
B
A
商品
物流ラベル
h．物流ラベルと認証情報による認証
受取者携帯端末
4b

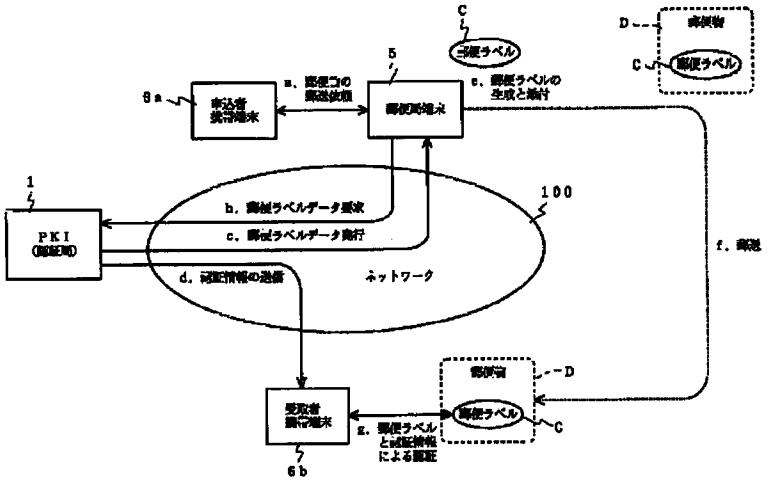
【図7】


申込者操作端末
物流業者
S21
商品の選択
S22
S23
S24
S25
S26
S27
S28
S29
S30
S31
S32
商品配送

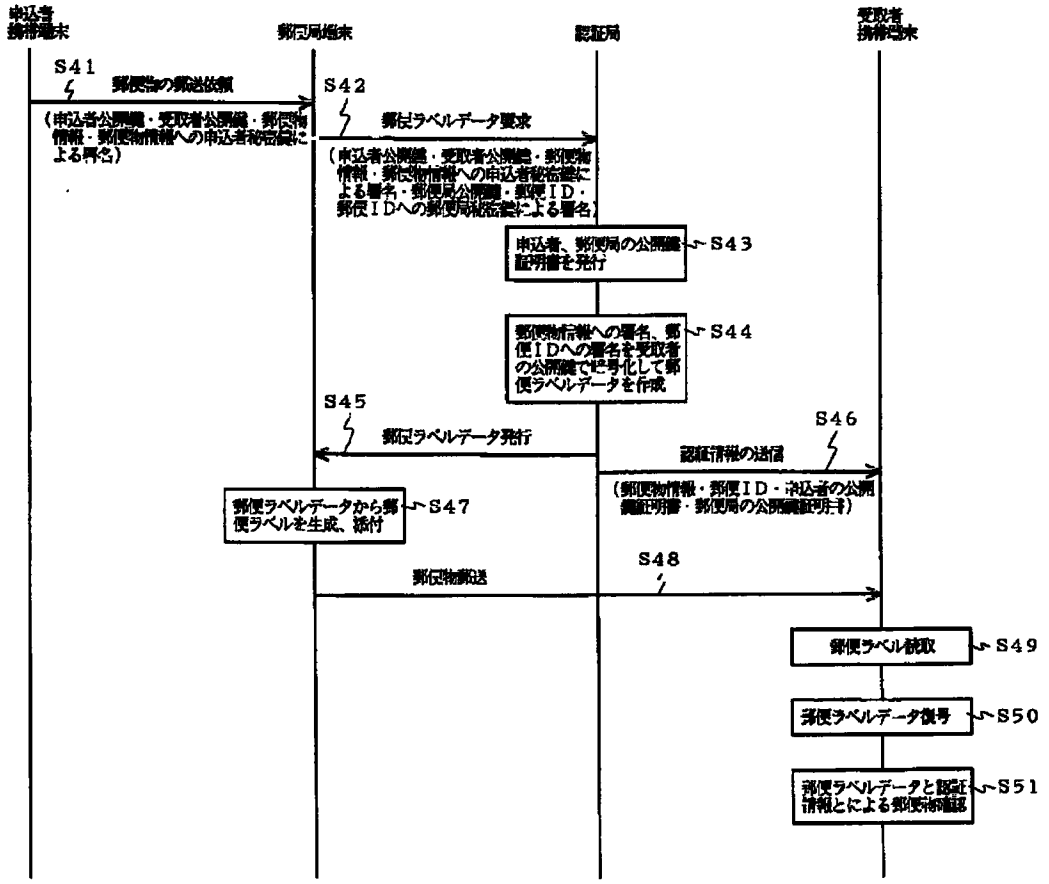
【図10】


申込者携帯端末
店舗端末
認証局
物流業者
受取者携帯端末
S21
商品の購入
(申込者公開鍵・受取者公開鍵・商品情報・商品情報への申込者秘密鍵による署名)
S22
物流ラベルデータ要求
(申込者公開鍵・受取者公開鍵・商品情報・商品情報への申込者秘密鍵による署名・店舗公開鍵・注文ID・注文IDへの店舗秘密鍵による署名)
申込者、店舗の公開鍵証明書を発行
S23
商品情報への署名、注文IDへの署名を受取者の公開鍵で暗号化して物流ラベルデータを作成
S24
S25
物流ラベルデータ発行
S26
認証情報の送信
(商品情報・注文ID・申込者の公開鍵証明書・店舗の公開鍵証明書)
物流ラベルデータから物流ラベルを生成、添付
S27
S28
商品配送依頼
S29
商品配送
物流ラベル読取
S30
物流ラベルデータ復号
S31
物流ラベルデータと認証情報とによる商品確認
S32
S33
物流ラベルデータ+受取情報送信

【図11】


C
D
C
8a
5
a.
e.
1
100
b.
c.
d.
ネットワーク
f.
D
C
g.
6b

【図15】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		(参考)
G06K	7/00		G06K	7/00	U
	17/00			17/00	L
					T
	19/00		G09F	3/00	ZECM
	19/10		H04L	9/00	675D
G09F	3/00	ZEC			675B
H04L	9/32		G06K	19/00	Q
					R

Fターム(参考) 5B035 AA13 BB01 BB09 BB11 BC00 CA23
5B058 CA15 KA02 KA06 KA11 KA35 YA20
5B072 BB00 CC06 CC24 DD01 GG01 GG07
5J104 AA10 KA05 MA01 PA10